联系我们

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

关注官方微信公众号　关注官方微信服务号　关注官方微信视频号　关注官方抖音号

亿赛通

ESAFENET

ESAFENET

亿赛通企业月刊　中国数据安全专家　www.esafenet.com

10月刊

2023 年共 12 期

亿赛通入选《北京市第一批商业秘密保护示范基地入选名单》，积极推进商业秘密保护新发展

亿赛通连续两年位列数据安全服务企业三甲

政策速递 | 数据跨境合规要求进一步明确：重要数据、个人信息出境合规问题有了新答案

数据交换：如何搭建企业隔离网间的安全桥梁？

亿赛通数据安全运营管理平台 | 某国际运营商典型案例

关注企业官方微信

Esafenet
Monthly magazines

中国数据安全专家

主办：亿赛通市场部

北京亿赛通科技发展有限责任公司

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

目录 CONTENTS

刊首语 PREFACE

《亿赛通十月刊》深入探寻数据安全治理的应用指南

随着数字技术和人们生活的交汇融合，数字化转型的深入发展，各类数据迅速增长、海量汇聚，数字安全对经济发展、社会安全、民生发展产生重大深远的影响。同时伴随着各项法律条文相继发布实施，我国数据安全发展正式迎来体系化建设“合规”时代。随着数字经济的蓬勃发展和数字中国建设的不断推进，加强数据安全治理已经成为时代的客观需要。在此期间，亿赛通不断深耕数据安全领域，持续探索完善最佳实践，助力各行业客户数字化转型，推动数字产业高质量发展，全力支持数字中国建设工作。《亿赛通十月刊》带你深入探寻数据安全治理的应用指南。

国内

1、D-Link 确认发生数据泄露，大部分属于低敏感度和半公开信息

摘要：本月初，有黑客在 BreachForums 上打包出售一份宣称是中国台湾厂商友讯科技（D-Link）的内部数据，要价 500 美元（当前约 3660 元人民币）。攻击者声称其中包括 D-View 网络管理软件的源码，以及三百万条涉及客户和员工个人信息的数据，其中甚至包括许多中国台湾地区政府官员和该公司 CEO 的详细信息。

2、电商经营者泄露百万条个人信息获刑，并支付公益损害赔偿金

摘要：在从事某电商平台经营过程中向他人无偿分享或有偿出售 100 多万条个人信息，造成大量客户被垃圾短信、推销电话骚扰——从南京市玄武法院获悉，该院近日判决揭某某等五人侵犯公民个人信息罪，判处有期徒刑三年至一年六个月不等，缓刑五年至二年不等，并处罚金，没收违法所得。鉴于他们损害了社会公共利益，法院还判决主犯揭某某等二人支付公益损害赔偿金 39600 元，在国家级媒体上赔礼道歉。

行业聚焦 INDUSTRY FOCUS

3、近 2 万条学员信息被泄露！黑客落网，培训机构被罚

摘要：福建厦门一培训机构系统，被“黑客”非法侵入，近 2 万条个人信息泄露，其学员更遭遇精准诈骗，厦门网警迅速出击，“黑客”落网获刑，该教育培训机构也因，未履行网络安全保护义务，被行政处罚，一起来看，同一教培机构学员，多人接到诈骗电话。

4、北京金融法院揭人脸识别诈骗套路 一女子泄露人脸信息后被诈骗分子转走 36 万余元

摘要：据北京金融法院审判第一庭法官甘琳介绍，近年来，随着信息技术的不断发展，人脸识别技术应用已经渗透到生活的各个方面。刷脸支付、刷脸打卡等人脸识别技术在为社会生活带来便利的同时，一些不法分子也开始利用人脸识别技术侵害金融消费者的合法权益。法官在审理的过程中发现，这些案件往往涉及民事和刑事程序的交叉，遭受损失的虽然是受害人，但是因为在泄露个人信息方面存在过错，所以在犯罪分子归案，非法所得追回之前，受害人可能无法通过民事诉讼获得有效的救济。特别是在金融交易领域中，商业银行等金融机构在为客户提供金融服务时所产生的金融信息，与个人的资产、信用状况高度相关，一旦泄露，很有可能会对个人的财产安全构成极大的威胁。这也就凸显出个人信息保护在参与金融活动中的重要性。

5、对业主个人信息保护不当，宁夏 6 家物业公司被处罚！

摘要：近日，宁夏石嘴山市 6 家物业公司因存在信息泄露隐患，被当地公安机关依法予以行政处罚。7 月 15 日以来，石嘴山市公安机关开展公民个人信息保护专项检查行动，严肃整治物业公司信息泄露乱象。检查中发现，多个物业公司办公电脑存储大量小区业主家庭住址、身份证号码、联系方式等个人信息，存储数据未经加密处理，办公电脑未设开机密码，对个人信息未实行分类管理、未采取加密及去标识化等技术措施，业主个人信息被泄露的风险极大。

6、演员陈牧驰离婚信息疑被泄露 律师：严重侵犯隐私权

摘要：最近，演员陈牧驰的个人生活引起舆论关注。特别是两张疑似民政部门婚姻登记系统截图，被广泛传播，其中涉及身份证号、户口信息等私密信息。律师表示，若网传截图为内部流出，发布者或触刑法。

7、便民“扫一扫”扫出广告链接，“数治”暗藏二维码风险

诈骗“链条” 新华社发 商海春 作

摘要：在西北某市一街道综合治理中心，半月谈记者看到工作人员正在通过公众诉求办理平台处理、反馈线上诉求。工作人员表示，数字化治理平台整合多项服务事项，二维码一扫即查、一点即看，提高了群众办事效率；街道社区通过收集信息数据、及时处理监测预警信息、办理交办诉求事件等，提升了日常工作的质效。时下，数字政府建设不断推进，多地创新推出各类便民服务二维码，以“数治”赋能“善治”，提升治理效能。然而，半月谈记者调研发现，由于便民服务二维码容易获得使用者信任，交互多，使用频率高，更易遭遇恶意利用或攻击，暗含安全风险。

8、员工拷走企业数据后跳槽！

摘要：近日，广西高院发布的一起案件判决引起社会关注。案件中，杨某在柳州一家机械公司任职近 10 年后，擅自拷贝公司 292 份文件，跳槽至该公司的竞争对手处，对原公司的商业机密构成了极大的威胁。最终，柳州市中院判决：杨某不得披露、使用、允许他人使用机械公司的商业秘密，并赔偿机械公司经济损失 1 万元。

9、出游高峰机票诈骗频发 谁泄露了旅客信息？

摘要：国庆假期出行高峰，个别旅客在网上订购了往返机票后，出发前收到“航班取消”等短信，提示旅客在支付软件中领取补偿，而当信以为真的旅客按“客服”要求下载指定 APP、开启屏幕共享，以及远程听取“客服”要求的一番操作后，却发现卡中的存款悉数清空。根据媒体报道，国庆前夕甚至有旅客因为“退改签”相关诈骗，损失了两百余万。反诈中心也持续发出预警，提示消费者注意此类骗术。

10、蜜雪冰城回应多地加盟商被骗：并非我方泄露信息

摘要：近日，河南郑州有商户反映加盟蜜雪冰城没过审，事后收到自称是代理商的私人微信消息，邀请加盟“子品牌”东芳叶。江苏昆山一加盟商称交完钱发现被骗，运营公司已经跑路。23 日，蜜雪冰城客服表示，不会泄露申请加盟的商户个人信息，所有提交的信息都会定期销毁处理。

国外

1、美国国税局前顾问认罪，承认泄露特朗普税务信息

摘要：据美国有线电视新闻网（CNN）报道，此前被美国司法部指控泄露特朗普税务信息的国税局前顾问查尔斯·利特尔约翰（Charles Littlejohn）当日在联邦法庭认罪，承认他在 2019 年和 2020 年窃取了特朗普和数千名其他富人的税务记录，并将窃取信息泄露给媒体。报道称，泄露纳税申报表和纳税申报信息的重罪指控最高可判处五年监禁，但出于检察官对量刑的考虑，利特尔约翰预计将面临 8 至 14 个月的监禁。

2、美媒爆料：特朗普曾向澳洲亿万富翁泄露美核潜艇敏感信息

摘要：据美国全国广播公司（NBC）6 日报道，根据美国广播公司（ABC）和《纽约时报》刊登的两篇报道，美国前总统特朗普在离开白宫后，据称向一名澳洲富翁泄露了有关美国核潜艇的敏感信息，而此人是特朗普名下私人俱乐部海湖庄园的会员。

3、基因检测巨头 23andMe 数百万用户信息遭黑客窃取，已在暗网出售

摘要：近日一些黑客窃取了美国基因检测巨头 23andMe 数百万用户的姓名、照片、出生细节和种族等数据，并在暗网上以数千美元的价格出售。23andMe 公司的一位发言人表示，这些数据似乎是通过之前泄露的用户凭证收集而来的，而 23andMe 公司的安全系统并没有被入侵。该公司是在 Reddit 上看到一篇帖子后才意识到这次攻击的，该帖子似乎已经被该平台删除，黑客们后来开始在网络犯罪市场 BreachForums 上兜售这些数据。

4、米高梅预计因黑客攻击导致数据泄露而损失 1 亿美元

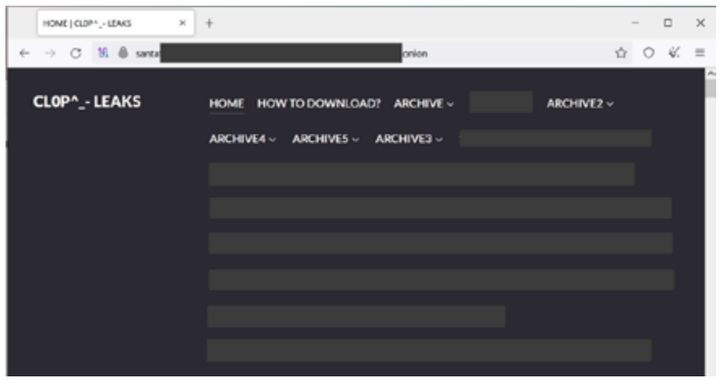
An exterior view of MGM Grand hotel and casino, after MGM Resorts shut down some computer systems due to a cyber attack in Las Vegas, Nevada, U.S., September 13, 2023. REUTERS/Bridget Bennett/File Photo Acquire Licensing Rights

摘要：米高梅国际酒店集团表示，上个月的一次网络攻击中断了该公司的运营，将对其第三季度业绩造成 1 亿美元的损失，并预计今年 10 月的总入住率为 93%，而去年同期为 94%。

5、威胁分子通过多条攻击链大肆利用 Progress WS_FTP 漏洞

摘要：从 2023 年 9 月 30 日开始，SentinelOne 观察到一伙威胁分子利用 Progress 的 WS_FTP 最近披露的漏洞，攻击运行该软件高危版本的 Windows 服务器。两个最严重的漏洞是 CVE -2023-40044 和 CVE -2023-42657，CVSS 评分分别为 10 分和 9.9 分。

6、CL0P 组织利用 Seed 传输窃取的敏感数据



摘要：CL0P 是 2023 年最活跃的勒索软件组织之一，仅次于 LockBit，在最近 10 个事件响应样本中，研究人员均观察到了 CL0P。CL0P 勒索软件组织在成功窃取了数千家公司的数据后，开始使用 torrent 来传播受害者数据。CL0P 的 torrent seed 基础设施为研究人员提供了一个独特的机会，让研究人员深入了解了臭名昭著的勒索软件组织的直接运行方式，并深入了解他们的交易技巧。通过分析托管被盗数据的现有 torrent seed 基础设施，研究人员可以更好地了解这一变化的含义。

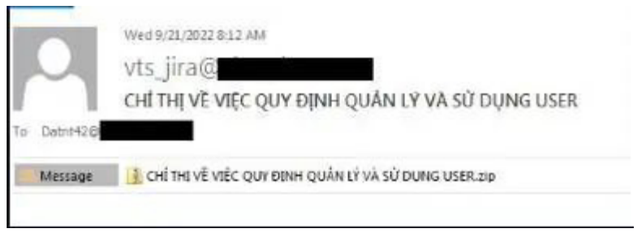
7、黑客冒充 Meta 招聘人员，针对航空公司进行攻击

摘要：拉扎罗斯集团（Lazarus Group）是一个与朝鲜有关的黑客实体，最近在针对西班牙一家航空航天公司的网络间谍攻击活动中被发现。此次发生的攻击事件是名为 " Operation Dream Job" 的更广泛的鱼叉式网络钓鱼活动的一部分，其攻击方式是以诱人的工作机会吸引潜在的具有战略意义的员工，从而进行整个感染过程。在媒体最近分享的一份技术报告中，ESET 安全研究员揭示了这次攻击的来龙去脉。在今年 3 月发生的一起事件中，这家斯洛伐克网络安全公司发现了一次针对 Linux 用户的攻击，通过利用虚假的汇丰银行工作机会部署了一个名为 SimplexTea 的后门。

8、ShellTorch 漏洞影响数万 PyTorch 模型服务器

摘要：研究人员在 TorchServe 中发现多个高分漏洞，影响数万 AI 服务器。TorchServe 是由 Meta 和 Amazon 负责维护的开源的 PyTorch 模型服务库，可大规模部署经过训练的 PyTorch，无需编写自定义代码，被学术界和产业界广泛应用于人工智能模型训练和开发，包括亚马逊、OpenAI、特斯拉、Azure、谷歌、Intel 等。

9、STAYIN’ ALIVE ——针对亚洲电信和政府部门的针对性攻击



摘要：在过去的几个月里，Check Point Research 一直在追踪分析“STAYIN’ ALIVE ”，这是一项至少从 2021 年就开始活跃的持续活动。该活动在亚洲开展，主要针对电信行业和政府机构。“Stayin’ Alive”活动主要由下载和加载程序组成，其中一些被用作针对知名亚洲组织的初始攻击载体。发现的第一个下载程序名为 CurKeep，目标是越南、乌兹别克斯坦和哈萨克斯坦。

10、索尼数据被黑客窃取并在暗网上进行出售

摘要：索尼公司再次陷入网络攻击的漩涡。这次是一个名为 "Ransomed.vc " 的黑客团伙，他们声称已经成功入侵了这家科技巨头的网络，该团伙声称，他们的目标是在黑市上出售被窃取的数据。 在本周早些时候，Ransomed.vc 大胆地宣称它已经进入了 " 索尼的所有系统 "，并准备出售被盗数据，据称是由于索尼 " 不愿意支付 " 赎金。该组织更进一步警告说，如果到 9 月 28 日星期四还没有买家出现，他们可能会开始公布被盗的信息。尽管目前这些指控是十分严重的，但我们必须要认识到它们目前仍未得到证实。

亿赛通入选《北京市第一批商业秘密保护示范基地入选名单》，积极推进商业秘密保护新发展

商业秘密直接关乎着企业的经营安全和竞争优势，对企业的重要意义已不言而喻。近年来商业秘密侵权纠纷日益频发，一方面反映出商业秘密已成为企业参与市场角逐的重点，另一方面则暴露出大部分企业因商业秘密保护制度的缺失或不完善所导致的维权困境。

近日，北京市市场监督管理局经过对各区推荐的近百家候选单位进行内部评选和专家评审，发布了《北京市第一批商业秘密保护示范基地入选名单》的企业名单公告。亿赛通在众多竞争者中脱颖而出，入选《北京市第一批商业秘密保护示范基地入选名单》。

商业秘密保护示范基地为打造一批示范引领作用突出、示范效果明显的商业秘密保护标杆企业、园区或社会组织，由市场监管部门组织企业、科研院所、产业集聚园区、特色产业基地、特色小镇等单位或社会组织建设的商业秘密保护示范点和商业秘密保护示范区。

其中，商业秘密保护示范点以高精尖产业（先进制造业、软件和信息服务业、科技服务业）为核心，兼顾其他产业，优先选取其中技术实力具有优势地位、商业秘密保护需求迫切、商业秘密保护意识强、商业秘密保护工作较为突出的单位作为培育对象。

亿赛通在商业秘密保护方面的贡献有目共睹，众所周知目前国内商业秘密保护意识、安全技术防护手段相对落后，标准需要完善，用户维权困难，管理模式需要更新，人才短缺。基于上述问题，亿赛通以“政策 + 标准 + 咨询 + 方案 + 服务 + 人才”相结合的“六位一体”发展思路，帮助合作企业增强商业秘密保护意识，完善商业秘密保护体系，提高商业秘密安全技术防护手段，系统化培养商业秘密保护人才，形成商秘保护管理新模式，为政策落地和企业赋能搭建一架专业的服务桥梁。

在 2022 年，亿赛通联合 20 余家成员单位共同发起成立中国开发区协会商业秘密保护专业委员会，这是公司在商业秘密保护提升服务功能的又一重大实践，同时也是亿赛通商业秘密保护进程上的重要里程碑。专委会赋能开发区企业数字化转型，切实保障园区企业的合法权益和创新活力。除此之外，我司还积极参与多项商业秘密保护相关标准及白皮书编制，希望通过建立统一的商业秘密安全保护技术标准，形成商业秘密保护技术的基本统一要求，提升企业商业秘密的安全性及对商业秘密的管理与保护能力，为商业秘密权利人和相关主体的合法权益提供规范性依据。

商业秘密是企业竞争力的核心，对企业发展至关重要。着眼未来，亿赛通将继续发挥自己的优势，加大产品研发，把握商业秘密保护市场，夯实基础，努力为用户提供优质的安全服务，为中国数据安全产业的健康可持续发展贡献出自己的一份力量！

亿赛通数据安全运营管理平台 | 某国际运营商典型案例

客户简介

某运营商作为全球最大的电信服务提供商之一，在全球拥有 50 条海缆，其跨洲容量 117T，建设的海外 PoP 节点达 229 个。其一直坚持深耕全球市场，致力满足全球客户日新月异的需求。为了配合近年全球企业急速的数字策略，该运营商为国际运营商、跨国企业和海外中国客户提供全方位、高质量的综合信息服务解决方案，並透过全面增强 DICT、云改数转及营运安全等关键能力，助力千行百业全速迈向数字化转型的旅程，携手于数字经济下寻找崭新机遇。

需求背景

近年来，国内数字经济和信息产业蓬勃发展，5G、大数据、人工智能、区块链等技术不断落地应用。新业态新技术在推动经济转型升级的同时，数据规模不断扩大，数据泄露、滥用等风险日益凸显，防范数据安全风险、构建数据安全保护体系成为各方共识。在此背景下，某国际运营商公司为抵御各类自动化攻击，全面提升自身核心应用、业务数据风险防范能力，构建面向数字时代的新一代主动防护数据安全体系，启动总部数据安全扩容项目。

存储数据安全风险

目前公司终端、文件存储服务器、数据库存在大量数据，需要加强对文档服务器、数据库和终端数据中的敏感信息识别能力。

敏感数据分类分级

对识别数据进行进一步梳理，形成数据资产台账，补足目前在非结构化数据板块的数据梳理能力，同时依据敏感数据识别规则和数据分类分级标准，对数据进行分类分级打标与重要数据标识。

终端数据安全风险

加强对终端数据的防泄露和加密防控，实现终端数据产生、使用、传输等生命周期安全管控，降低内部核心数据泄露风险，提升终端数据安全管控能力。

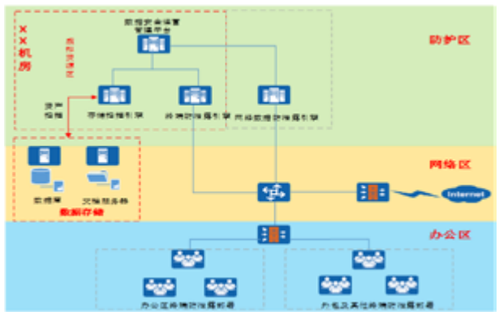
数据防泄露统一运营

加强对敏感数据资产的掌控，做好公司内部数据溯源的技术铺垫，构筑严密的防泄露技术工事，做到事前预防、事中控制、事后溯源，全程态势感知的数据安全防护闭环，为此需要在一期网络数据泄露防护的基础上再次进行终端数据防泄露、存储数据防泄露、数据安全统一平台的建设。

解决方案

新建数据安全统一管理平台，虚拟化部署。平台支持结构化与非结构化数据分类分级，接入终端数据防泄露、网络数据防泄露、存储扫描数据防泄露，实现终端、网络、存储 DLP 同平台管理，同时支持各模块日志进行运算分析，实现安全态势大屏、资产统一管理、设备统一运维、策略统一下发、风险统一处理、趋势行为分析、事件智能分析、事件追踪溯源等能力。

利旧现有的网络数据泄露防护系统，将网络数据泄露防护系统接入统一管控平台进行统一管理，并将网络数据、终端数据进行关联分析，形成终端到网络的立体式防护。



敏感数据发现

运营管理平台基于自动扫描、网络探测、手动添加等多种方式对网络环境中的资产进行梳理并形成数据资产目录，帮助用户梳理数据资产台账、厘清数据资产、降低数据资产管理难度。

数据分类分级

在识别敏感信息的过程中依据 YD/T 3813-2020《基础电信企业数据分类分级方法》并结合公司已有的数据分类分级规范，对识别的数据进行进一步梳理，形成数据资产台账，同时按照 YD/T 3867-2021《基础电信企业重要数据识别指南》对分类分级后的数据进行重要数据标识。

数据外发管控

根据敏感数据发现形成的分类分级清单，对办公区终端、外包和其他运维终端安装部署的终端探针进行策略部署与下发，按照数据的敏感类型与重要程度实施不同的管控强度。

数据安全运营

通过运营管理平台对终端数据安全、网络数据安全、存储数据安全进行统一监控、统一运维、智能分析、态势感知，构建覆盖“端 - 网 - 业务 - 存储”的可视、可管、可控、可溯能力。

方案价值

01、安全联防联控

通过统一运营管理平台实现对项目一期网络数据安全建设与二期终端及存储数据安全建设的联防联控。

02、数据分级防护

不同级别数据采用不同的技术防护，实现分级、精准化防护，实现安全与效率最大平衡。如 4 级、3 级数据进行存储加密保护，2 级数据进行访问权限控制，1 级数据进行流转监测审计。

03、全网数据分析

终端事件数据、网络事件数据、存储扫描事件数据同时上报至运营管理平台进行综合分析，形成全网数据溯源能力。

亿赛通连续两年位列数据安全服务企业三甲

2023 年 10 月 26 日，中国互联网协会（以下简称协会）在厦门举办中国互联网企业综合实力指数（2023）发布会暨百家企业论坛。会上，协会正式发布了 2023 年数据安全服务前五家企业名单，亿赛通凭借专业的数据安全服务，连续两年位列三甲且排名逐年递增，2023 年排名第 2。

自 2013 年以来，协会已连续 11 年开展中国互联网企业综合实力研究工作，详实展现了中国互联网企业总体的发展现状与态势，系统反映了我国互联网行业未来发展趋势，获得了政府部门、行业机构、业界专家的广泛关注和认可。

本次除了入选数据安全服务榜单外，北京亿赛通科技发展有限责任公司副总经理张兰兰作为特邀嘉宾在会中发表了主题为“企业数据安全治理智能化体系建设方案”的演讲。数据自 2019 年起首次增列为一种生产要素，此后随

着各项政策条款的颁布，数据要素成为重要国家战略，进而国家、企业对数据安全的重视逐步加深。技术、产品和服务是数据安全产业的关键要素，其发展水平直观体现了产业的发展状况。在政府、企业、社会的多方推动下，我国数据安全技术、产品体系逐步完善，数据安全服务发展态势良好。综合来看，我国数据安全已迈入飞速发展的关键时期，在给供给侧带来发展机遇的同时，也对数据安全服务质量与产品技术能力提出了更高的要求。

亿赛通在业内提出“分·放·管·服”数据安全建设理念，从制度层和技术层同时入手，制度主建指导数据安全体系建设，做到有规可依；技术主战保障制度实施，做到有规必依，违规必纠；通过技术不断发现风险补制度漏洞，优化制度，通过制度对技术创新提要求，形成制度和技术的循环优化闭环。

亿赛通“分放管服”数据安全建设理念

再针对瞬息万变的安全风险，亿赛通提出了综合数据安全治理一站式解决方案。通过智能化、自动化工具引擎对业务与数据进行梳理，形成人与数据间的安全策略并导入到安全运营组件。运用独特的安全服务 + 安全产品 + 平台运营的理念为客户提供数据安全体系化服务。从业务梳理、分类分级、策略制定、技术管控等方面帮助客户建立全方位的数据安全体系建设。

在企业进行数据安全治理的过程中，亿赛通数据安全运营管理平台作为重要的服务支撑能力，将各个孤立的安全系统进行资源整合，实现数据资产可视、数据威胁可管、数据风险可控、数据血缘可溯。平台通过对全网数据进行综合分析，形成用户身份画像，可了解在一定时间段的用户数量、活跃用户、高风险用户，以及用户的操作行为。基于以”人“为中心的关联分析技术，分析可疑人员在云、网、端的所有操作行为、操作对象、目标地址、以及与之关联的其他人员，通过将主体和客体关联形成全网数据关联分析能力。用户的行为操作经过各个节点的审计记录后，由平台对采集的事件日志进行合并、关联分析，将事件的整个操作过程以数据为中心节点进行还原，形成有效的溯源证据链。实现与各个安全能力组件的联动，覆盖云、网、端、各个节点的立体化管理。

数据安全运营管理平台

随着我国数字经济的稳步发展，新一代信息技术已经成为引领创新和驱动发展的动力源，为稳经济、惠民生、增活力、促发展发挥重要作用。而作为我国数据安全领域的先锋，亿赛通也将继续发挥自己的优势，把握数据安全发展机遇，夯实基础，持续向用户提供优质的安全服务，为中国数据安全产业的健康可持续发展贡献出自己的一份力量！

政策速递 | 数据跨境合规要求进一步明确：重要数据、个人信息出境合规问题有了新答案

2017 年 6 月 1 日，《中华人民共和国网络安全法》实施，第三十七条明确提出“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估”。2021 年 9 月 1 日，《中华人民共和国数据安全法》施行，第三十一条新增“其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定”。同年 11 月 1 日，《中华人民共和国个人信息保护法》生效，明确了个人信息出境场景下的三条合规路径。至此，以重要数据和个人信息为核心的出境监管要求正式确立。在上位法指导下，《数据出境安全评估办法》《个人信息保护认证实施细则》《个人信息出境标准合同办法》等文件接连发布，为进一步落实监管要求提供了实施指引。

近一年来，相关企业积极排查跨境业务，判别适合自身的合规路径，基于监管要求制定、落实整改方案。北京、上海、浙江、江苏等区域的企业向主管部门提交数据出境安全申报材料并完成审批，数据出境安全评估项目已陆续落地。但同时，企业在合规治理工作中也面临拟出境数据中重要数据难识别，100 万以上个人信息处理者即使出境少量个人信息也需要进行出境安全评估，从而影响跨境业务效率等问题。2023 年 9 月 28 日，网信办发布《规范和促进数据跨境流动规定（征求意见稿）》（以下简称《规定》），针对这些问题给予了澄清和细化。

《规定》主要内容如下：

01 再次强调，不涉及重要数据和个人信息的数据可自由出境。

《规定》第一条指出，“国际贸易、学术合作、跨国生产制造和市场营销等活动中产生的数据出境，不包含个人信息或者重要数据的，不需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。”亿赛通在为企业提供数据跨境合规咨询服务的过程中，一些开展跨境业务的企业对我国数据跨境监管目标、监管范围不甚明确，较难判定拟出境的数据中是否包含需要进行合规申报的数据，可结合《规定》中的此条内容，对拟出境数据分类分级，将重要数据和个人信息依照合规要求单独识别和保护，将不涉及重要数据和个人信息的数据放心出境。

02 进一步明确，数据出境场景中是否涉及重要数据需要由国家“相关部门或地区”认定。

《规定》第二条指出，“未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。”自数据安全法构建了重要数据保护制度以来，各类组织在数据分类分级、数据安全评估、数据出境合规管理工作中都避免不了要进行重要数据识别的工作。但是国家标准《重要数据识别规则》一直未正式发布，各行业重要数据目录的制定工作也刚刚开始，重要数据保护制度的落地面临困难。此条目针对数据出境这一重要场景，提出只有被告知或公开发布为重要数据的相关数据出境才需要进行数据出境安全评估申报，在重要数据识别规则不明朗的现阶段，可一定程度上帮助企业规避重要数据识别困难的问题。但是，仍建议相关机构审慎考量拟出境的数据范围，密切跟进行业重要数据目录等相关文件的制定进度，对“疑似重要数据”积极识别、保守出境。

03 进一步澄清，向境外提供个人信息的高效、便利化监管条件。

之前，个人信息保护法等针对向境外提供个人信息的场景，已经明确了个人信息出境安全评估、标准合同、保护认证三条合规路径。但相关企业在合规治理工作中，仍面临一些个人信息出境场景是否属于合规监管范畴的难题。《规定》针对此类问题进一步明确：

（1）向境外提供不属于在境内收集产生的个人信息，不需要走三条合规路径。一些企业在从事跨境业务中，不乏数据从境外采集过来，在境内存储一段时间后又传输到境外，或者从境外采集的数据在境内存储过程中被境外调用的场景，此条目强调，如果可证明这部分数据不属于在境内收集产生，且没有经过境内主体的处理，则无须走三条合规路径；如果在境内存储过程中经过了境内主体的处理，则要判断数据处理过程是否涉及国家核心技术等，以防止该部分数据向境外提供构成影响我国国家安全或公共利益的隐患。

（2）跨境购物等个人信息主体自主发起的个人信息出境行为、依照制度或合同实施人力资源管理工作所必须、紧急情况下需要向境外提供个人信息以保护他人生命财产安全的，不需要走三条合规路径。首先，跨境购物、跨境汇款、机票酒店预订、签证办理等，个人信息主体按照自己的意愿主动发起，或者自然人因个人或者家庭事务处理个人信息的，不适用于数据跨境监管要求。其次，跨境企业内部进行人力资源管理，依照依法制定的劳动规章制度和依法签订的集体合同进行个人信息跨境传输的，不适用于数据跨境监管要求。最后，紧急情况下为了保护个人生命健康、财产安全等利益所必须向境外提供个人信息的，不适用于数据跨境监管要求。这也是《规定》在数据跨境场景中进一步细化个人信息保护法第十三条、第七十二条的表现。

（3）预计一年内向境外提供不满 1 万人个人信息的，不需要走三条合规路径；预计一年内向境外提供 1 万人以上、不满 100 万人个人信息，可选择标准合同或个人信息保护认证。国家机关和关键信息基础设施运营者向境外提供个人信息的，依照有关法律、行政法规、部门规章规定执行。

按照先前文件要求，关键信息基础设施运营者和 100 万人以上个人信息处理者，只要向境外提供个人信息，就需要申报个人信息出境安全评估。即，这类主体即使出境一条个人信息，也需要进行相应评估和申报。数据出境安全评估

相比其他两条合规路径，程序更为复杂，要求更为严格。此条规定的发布，从源头处进一步把控了数据出境安全评估的适用范围，大大降低了这类主体的数据跨境合规成本，是我国探索便利化的数据跨境流动安全管理机制的具体体现。同时，《规定》第八条明确，关基运营者向境外提供个人信息，仍按照关基保护等相关制度执行，在保障跨境流动便利机制的同时，对特殊群体的数据安全管理工作进行了兜底性约束。

（4）不适用三条合规路径的个人信息出境行为，仍需开展个人信息保护影响评估工作。

依照个人信息保护法第五十五条，向境外提供个人信息的个人信息处理者，应当事前进行个人信息保护影响评估。因此，即使不受三条合规路径的监管，将要向境外提供个人信息的个人信息处理者也应参照数据安全风险评估相关标准要求开展相应的评估工作。

04 首次提出，由自贸区自行制定“负面清单”，“负面清单”以外的数据可以自由跨境流动。

8 月 13 日，国务院印发《关于进一步优化外商投资环境加大吸引外商投资力度的意见》提出，“试点探索形成可自由流动的一般数据清单”。此条目可理解为对这项政策的回应。在实践中，数据出境场景频繁，相比大量不危及国家安全、公共利益、个人隐私保护权益的一般数据跨境行为，受国家重点监管的数据和场景有限。因此，从制定受限场景下（即适用于三条合规路径）的数据清单为抓手，以自由贸易区为试点，探索数据自由跨境流动管理模式，是我国优化外商投资环境、高效构建数据跨境流动管理机制的又一举措。

《规范和促进数据跨境流动规定（征求意见稿）》就相关机构关心的多个数据出境场景下的安全评估、签署出境标准合同、通过个人信息保护认证的义务予以豁免，如

获颁布，将大幅降低机构的数据出境合规成本，是国家探索便利化的数据跨境流动安全管理机制的重要体现。

亿赛通深入研究相关政策法规文件精神，致力于为相关机构提供数据出境合规咨询服务，通过建立出境合规管理机制、数据出境业务分析、拟出境数据分类分级、数据出境安全合规评估、出境方数据安全能力论证、数据出境合规整改、境外方数据安全能力论证、编制数据出境安全合规评估报告、出境行为和风险持续监测九个步骤，帮助相关企业落实数据出境监管要求，掌控敏感数据流向，完善数据安全体系化能力，从而最终实现数据资产的放心流转，加强关联主体间的信息共享，保障出境业务的高效流通。

数据流通：如何打通数据全生命周期的“任督二脉”？

发展数字经济，需要在万物数字化的基础上，充分挖掘释放蕴藏在数据中的价值，数据的开发和应用能力已经成为体现一个国家、地区或组织综合竞争力的关键指标。数据价值的发挥依赖于多元数据的融合、分析与应用，只有数据流通起来、用起来才能产生价值、发挥作用。而数据全生命周期的每个阶段涉及众多利益相关者，只有充分发挥各阶段利益相关者的积极性，全面保障各阶段利益相关者的权益，才能实现数据流通的价值最大化，形成健康的数字经济生态。

数据流通是释放数据要素价值的关键一环。一方面，数据具有外部性，即同一组数据可以在不同的维度上产生不同的价值和效用。借助数据流通数据可以在不同的数据接受者一方与自有数据汇聚，不断开拓使用维度，数据价值也将在社会面层层放大。另一方面，数据存在分布不均衡的问题，企业采集的数据通常具有较强的行业属性，特征不够全面，同时中小型企业收集的数据样本量较少，难以支撑业务。数据流通为利用数据的外部性，解决数据分布不均衡的问题，充分释放数据要素价值提供了有效手段。

据某咨询机构报告显示：国内数据流通安全整体市场规模 25.5 亿元。随着数据流通的方式和路径日益复杂，数据流通需要综合考虑多方面因素，未来需要深化数据要素流通工具、打造数据共享交换平台、全球化布局数据流通安全规模并采用具有多重安全措施和防范控制机制，以确保数据的安全流通。

现阶段，从数据安全角度，数据流通的主要方式有数据访问控制、数据交换、数据跨境等。由于数据流通存在技术依赖、非标准化的特点，面向多元数据主体和多样数据流转形态，参与流通的供需双方需要科学、可靠且共识的规则体系，才能建立信任。现阶段，从政策指引到应用实践，各方均在积极探索建立健全数据流通规则。在政策指引方面，《关于构建数据基础制度更好发挥数据要素作用的意见》中明确要建立合规高效的数据要素流通和交易制度，完善数据全流程合规和监管规则体系，建设规范的数据交易市场。在实践探索方面，各地方、各行业、各类市场主体也在实践过程中积极探索数据流通配套规则。其中，金融行业以 28.5% 的占比远远高于其他行业，互联网、政务、运营商行业紧随其后。

亿赛通基于二十年数据安全实践经验，将数据细分为对结构化、非结构化和半结构化，基于云、网、端三类场景对电子文档、数据库进行全方位、多维度、全生命周期的管理。结合“分放管服”数据安全建设理念，在分类分级，数据书里的基础上，依据差异化的数据安全策略，落实“低敏感数据放行流通”“高敏感数据受控使用”的工作原则。即在终端层，基于数据内容进行全量、增量、定期、周期性扫描，对数据进行识别与检测，按照数据分类分级标准制度对数据

进行分类分级管理，实现加密、外发审计、审批和阻断管理等措施；在网络层内置全球 IP 地址库，将数据访问发起端和响应端进行 IP 地址比对，识别数据的违规流转、跨境传输、非法出境状态记录、风险告警及流转阻断限制；在数据分散存储时，在终端、服务器端、云虚拟环境、网络端、邮件端可进行全覆盖多点部署，有力保证企业的数据安全建设。

强化全生命周期的数据安全保障能力，数据要素需要有效、安全的流通，才能推动传统业务的变革，做到数据价值最大化。亿赛通将积极发挥技术优势与经验沉淀，用高性能的产品与高品质的服务，为数据经济高速发展保驾护航。

政策解读 | 《工业和信息化领域数据安全风险评估实施细则（试行）》（征求意见稿）

数字经济时代，数据作为重要的新型生产要素，在不断流通的过程中，充分释放数据价值的同时，也面临着诸多安全风险与挑战，数据安全风险评估是做好数据安全建设的重要一环。《数据安全法》第三十条规定：重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。《工业和信息化领域数据安全管理办法（试行）》（以下简称《管理办法》）第三十一条规定：工业和信息化领域重要数据和核心数据处理者应当自行或委托第三方评估机构，每年对其数据处理活动至少开展一次风险评估，及时整改风险问题，并向本地区行业监管部门报送风险评估报告。

为贯彻落实《数据安全法》《工业和信息化领域数据安全管理办法（试行）》等法律法规、政策文件有关数据安全风险评估的相关要求，进一步细化工业和信息化领域数据安全风险评估规则，规范风险评估活动，有效提升重要数据和核心数据保护水平，2023 年 10 月 9 日，工信部发布《工业和信息化领域数据安全风险评估实施细则（试用）》（征求意见稿）（以下简称《实施细则》）。

本次发布的《实施细则》征求意见稿共十七条，明确了部省两级数据安全风险评估工作体系，细化了重要数据和核心数据处理者的评估义务，明确了行业主管部门监督管理评估活动的机制流程。主要内容包括：

1、明确了适用对象为工信领域重要数据和核心数据处理者

第二条明确：该细则适用于中华人民共和国境内工业和信息化领域重要数据和核心数据处理者开展的数据安全风险评估活动。一般数据处理者可参照本细则开展数据安全风险评估。

关于重要数据和核心数据的界定，可以参考《管理办法》第十条和第十一条的相关规定。

第十条 危害程度符合下列条件之一的数据为重要数据：

（一）对政治、国土、军事、经济、文化、社会、科技、电磁、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等与国家安全相关的重点领域；

（二）对工业和信息化领域发展、生产、运行和经济利益等造成严重影响；

（三）造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大；

（四）引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响；

（五）经工业和信息化部评估确定的其他重要数据。

第十一条 危害程度符合下列条件之一的数据为核心数据：

（一）对政治、国土、军事、经济、文化、社会、科技、电磁、网络、生态、资源、核安全等构成严重威胁，严重影响海外利益、生物、太空、极地、深海、人工智能等与国家安全相关的重点领域；

（二）对工业和信息化领域及其重要骨干企业、关键信息基础设施、重要资源等造成重大影响；

（三）对工业生产运营、电信网络和互联网运行服务、无线电业务开展等造成重大损害，导致大范围停工停产、大面积无线电业务中断、大规模网络与服务瘫痪、大量业务处理能力丧失等；

（四）经工业和信息化部评估确定的其他核心数据。

2、明确工信部、地方行业监管部门的职责分工

第三条规定，由工业和信息化部统一管理、监督和指导工业和信息化领域数据安全风险评估工作，组织开展相关评估标准制修订及推广应用。地方行业监管部门，包括省级工信主管部门、省级通信局和无线电管理机构，依据职责分别负责监管本地区工业、电信、无线电领域的重要数据和核心数据处理者开展风险相关评估工作。

之前的《管理办法》明确了工信领域数据包括工业数据、电信数据和无线电数据，并对相关概念进行了界定，具体可参见《管理办法》第三条。

3、明确了数据安全风险评估要素和评估内容

第五条明确：评估要素为数据处理活动的目的和方式、管理体系、技术工具、人员能力、风险影响等，并按照以上要素细化了具体评估内容，包括：

评估要素	评估内容
目的方式	数据处理目的、方式、范围合法、正当、必要
管理体系	数据安全管理制度、流程策略
	数据安全组织架构、岗位配备和职责履行
技术工具	数据安全技术防护能力建设及应用情况
人员能力	数据处理活动相关人员情况
数据跨主体处理	涉及数据跨主体处理的，数据提供方、接收方的安全保障能力、诚信守法和责任义务约束情况
数据出境评估	涉及数据出境评估的，履行数据出境安全评估要求落实情况及与申报事项的符合情况

4、提出了评估期限、重新申报评估的情形、可采取的评估方式

第六条明确：重要数据和核心数据处理者每年完成至少一次数据安全风险评估，并形成评估报告。数据安全风险评估结果有效期为一年，自评估报告首次出具之日起计算。

对于需要重新开展数据安全风险评估的情形包括：

（1）新增跨主体提供、委托处理、转移的；

（2）安全状态发生变化对数据安全造成不利影响的；

（3）发生涉及重要数据、核心数据的安全事件的；

（4）行业监管部门要求进行评估的其他情形。

第七条明确：评估方式包括两种，一是自评估；二是委托第三方评估，评估过程要求建立专业化评估团队、制定完整的评估工作方案，配有有效的技术评测工具。

5、对委托评估、风险控制和评估报告报送等作出要求

第八条至第十条对对委托评估、风险控制和评估报告报送等作出要求。

关于委托评估的要求，一是要签订合同或其他具有法律效力的文件；二是向第三方机构提供必须的材料，且材料要确保真实性和完整性；三是要确认评估结果。

关于风险控制的要求，要对评估中发现的数据安全风险隐患及时采取适当措施消除或降低风险隐患。

关于评估报送的要求，一是在评估工作完成后的 10 个工作日内，向本地区行业监管部门报送或更新评估报告；二是中央企业督促指导所属企业履行属地数据安全风险评估及评估报告报送要求，并将梳理汇总的企业集团本部、所属公司的评估报告报送工业和信息化部；三是地方行业监管部门将本地区本领域重要数据和核心数据处理者的评估报告报送工业和信息化部备案。

此外，第十一至十五条明确评估报告审核、评估机构认定、评估机构义务、监督检查、机构监管等要求。第十六至十七条明确行业监管部门及委托支撑机构的工作人员的保密义务，提出涉及军事、国家秘密信息等数据处理活动参照有关规定执行。

目前，我国也已经出台了一些关于数据安全风险评估的国家标准，可以用于指导风险评估工作的开展。2023 年 5 月，全国信安标委发布《网络安全标准实践指南—网络数据安全风险评估实施指引》，给出了网络数据安全风险评估的评估思路、工作流程和评估内容，提出从数据安全管理、数据处理活动、数据安全技术、个人信息评估安全风险。同年 8 月，全国信安标委发布国家标准《信息安全技术 数据安全风险评估方法》（征求意见稿），提出了数据安全风险评估的基本概念、要素关系、分析原理、实施流程、评估内容，明确了数据安全风险评估各阶段的实施要点和工作方法。这些文件为数据处理者、第三方机构开展风险评估提供了参考依据。

《实施细则》充分细化落实了《工业和信息化领域数据安全管理办法（试行）》第三十一条对于数据安全风险评估的要求，对指导工业和信息化领域数据处理者规范开展风险评估工作具有重要意义。工信领域重要数据和核心数据处理者应提高重视，结合《实施细则》相关内容及参照相关标准，积极开展数据安全风险评估工作。

请查收这份勒索病毒防护指南

纵观国内数据安全环境，传统行业数字化、网络化、智能化，暴露出一系列数据安全问题。勒索病毒也乘机发难，疯狂敛财，影响日渐扩大。机构企业成是勒索组织的首要攻击目标！有数据显示超过 80% 的勒索软件感染都是针对机构企业的。相比广撒网，更有选择性的攻击能为网络罪犯带来更多利益。据某勒索病毒分析报告显示，从行业角度分析，医疗、制造及芯片行业是勒索病毒攻击的重灾区，生活服务业紧随其后。勒索病毒通过计算机漏洞、邮件投递、恶意木马程序、网页后门等方式进行传播，整体攻击方式呈现多元化的特征。

近日，索尼证实被勒索攻击组织入侵了在线服务器，并窃取了超过 3.14GB 包含大量用户详细信息的数据。并且由于索尼公司不愿意配合谈判并按要求支付赎金，因此勒索组织将公开售卖这些“数据和访问权限”。

企业遭受勒索病毒攻击后，会造成服务器上的文件和数据全部被加密，且数据很难被恢复，即使支付高额的赎金，也很难保证全部文件和数据被还原。并且由于被迫中断业务，会给企业声誉造成严重影响。这类情况通常由于企业内网中各类操作系统的服务器与终端，存在很大的系统漏洞等风险，极易被侵入与提权。而且企业不重视数据安全的建设，等到真正出现安全事件时，造成重大损失，才想到要防患于未然。

数字经济的加速推进，也加剧了黑客对病毒进行迭代。大部分企业面对勒索攻击的手段如下：

- 不点击标题可疑的未知发件人邮件；
- 不随便打开电子邮件附件；
- 不随意点击电子邮件中的附带网址。
- 打开使用电脑的防火墙；
- 更新系统补丁 / 安全软件病毒库；
- 将数据备份在两种不同的存储类型，如服务器 / 移动硬盘 / 云端 / 光盘 / 磁带等；

但做到这些还远远不够，在亿赛通看来，想要有效规避突发性勒索病毒损失，做到事前主动防御，弥补传统防护手段的不足。基于对勒索病毒特性及网络安全建设现状等方面分析，推出产品 + 服务体系，以企业数据资产的保护为切入点，联合中国太平洋保险共同开展网络安全保险业务，由传统的“事后理赔”模式转变为 “事前防御、事中预警、事后补偿”的全新模式。太平洋保险公司设立“防勒索数据安全险”，针对高价值文件提供防勒索安全保障，这不仅是一份保障合同，更是一项专业责任的服务承诺。

保前安全监测

远程风险测评、制定各项重要数据的保密服务承诺，配备完善全面的保险应急方案。

保中安全监控

对数据进行风险监测、预警、发现问题第一时间通知管理人员，快速启动应急处理方案，及时降低安全风险。

保后应急响应

承诺 72 小时达到现场，定责定损，安全专家修复系统、恢复数据。

对于数据安全，没有准备就是准备没有！亿赛通针对数据全生命周期的多场景、高性能、智能化的安全治理需求，历经 20 余年的技术积累和上万个交付项目的沉淀，重点突破了端点数据自适应防护、海量数据内容审计、重要数据深

度感知、敏感数据智能防护等关键技术，授权了 50 余项发明专利，达到了国际先进水平，提出了数据安全“分放管服”建设理念和数据安全治理智能化体系，自主研制了电子文档安全管理系统、数据泄露防护系统、API 审计系统、数据库审计系统、数据库防火墙、数据库运维系统、数据脱敏系统、数据交换系统及文件防火墙等，覆盖了“云网端”等场景，构建了数据安全运营管理平台、数据安全态势感知平台及数据安全智能管理平台等。

最后再次提醒大家提高安全防范意识，做好数据安全防护和备份，如有任何需要可以拨打亿赛通客户服务热线电话：400-898-1617

数据隐私保护之数据脱敏的重要性

在数据要素成为企业重要资产的当下，对于企业不同的业务部门来说，每时每刻都在通过共享数据方式进行业务协作。一些企业会将大量的敏感客户数据拷贝到开发、测试、数据分析环境，但并没有采取任何对数据脱敏的措施。这将面临重大的监管及数据泄露风险。为了保证数据在企业内外部依法依规使用，需要相应的数据脱敏技术来实现对敏感数据的保护。

相关的法律法规、还有标准文件的出台，如：《中华人民共和国网络安全法》、《信息安全技术 个人信息安全规范》、《中国银行业“十二五”信息科技发展规划监督指导意见》、《银监会信息科技风险现场检查指南》中都有对数据去标识化，进行脱敏的规定。虽然在政策法规要求中，对于个人信息的保存和提供要经过匿名化处理，然而在正常生产和使用过程中，很多环节需要对敏感数据进行共享和使用，这时候都是存在一些数据泄露风险的场景，这些场景中数据脱敏是必经环节。法律法规和行业要求，对数据脱敏的时候有相应的脱敏程度要求，比如匿名化、去标识化，其中匿名化是对个人信息处理之后，使得个人信息主体无法被识别。去标识化是处理后不借助额外信息的情况下无法识别个人信息主体的过程。

数据的可用范围，正常情况下敏感数据是只能存在于生产环境中，经过脱敏之后就可以在测试环境中存储、在开发环境中存储以及对外部开放访问。敏感数据主要可能有个人隐私数据、企业业务数据，还有数据分级分类之后安全级别很高的核心数据。

还有脱敏涉及的数据源、数据类型，最早的数据源都是关系型数据库，尤其是数据类型部分以结构化的为主，后续也有了大数据体系的数据源，有了更多非结构化的数据。最早数据脱敏的主要是针对数值和文本这种很基本的数据类型，现在对于图片、对音频、视频都有脱敏的需要。

脱敏技术中两个比较重要的概念：静态脱敏及动态脱敏。静态脱敏简单说就是对数据进行批量化脱敏，一般用在测试开发或者是对外进行完整的数据集外发的场景中，主要特点是数据会发生批量的转移，静态脱敏这个技术可以视作是 ETL 过程中转换的步骤变成脱敏算法，整体跟 ETL 很像。

一、静态数据脱敏

静态脱敏应用的场景，主要为结构化数据或数据统计信息，数据集的可用性不能被破坏，这种情况适用于静态脱敏。

亿赛通静态数据脱敏系统（简称 :DMS-S），是一款面向敏感数据通过脱敏规则进行数据变形，实现敏感信息的可靠保护的数据脱敏产品。实现自动化发现源数据中的敏感数据，并对敏感数据按需进行脱敏规则变形，避免敏感数据泄露，脱敏后的数据保持了数据的一致性和业务的关联性，应用于开发测试环境、数据交换、数据分析、数据共享等场景。同时对脱敏过程进行监控审计，对数据敏感数据源、敏感数据类型、脱敏任务进行多维度的统计并进行图形化展现。

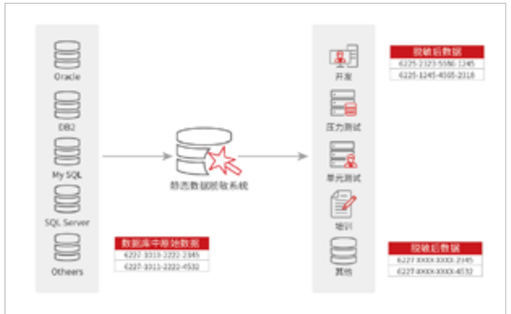
01、开发、测试使用场景

在开发、测试等场景当中，用户会使用到大量的数据，如果直接使用未经脱敏的生产数据，其一若涉及个人隐私数据则不合规，其二极易造成敏感数据泄露。

1. 静态脱敏系统根据不同数据特征，内置了丰富高效的脱敏算法，脱敏方案主要使用数据仿真、随机字符串、列关联的方式进行；

2. 不要求全量数据，根据开发测试环境的具体要求拟定脱敏方案；

3. 脱敏主要通过数据库到数据库的模式进行。



02、手工脱敏场景

企业中主要由内部相关人员进行手工或者编写简单的函数进行脱敏，占用大量人力和时间，且脱敏效率太低，导致数据大量失真，无法进行任务计划、断点续传等。

1. 静态脱敏系统根据不同数据特征，内置了丰富高效的脱敏算法，脱敏方案主要使用数据仿真、随机字符串、遮蔽的方式进行；

2. 可根据具体要求拟定相应的脱敏方案；

3. 脱敏主要通过数据库到数据库的模式进行。

03、数据外发场景

在数据外发场景中涉及业务数据接口调用和数据上报给第三方，在使用接口开放给第三方数据共享或者部分数据上报给外部的第三方或上游组织，若数据中包含未经脱敏处理的敏感信息，数据一旦泄露后果将会非常严重。

1. 静态脱敏系统根据不同数据特征，内置了丰富高效的脱敏算法，脱敏方案脱敏方案主要使用遮盖的方式进行；

2. 保证主外键一致、业务关联一致、有依赖字段的敏感信息脱敏一致、多次脱敏结果保持一致等，整体保证脱敏前后一致性，保持数据间的逻辑关系，数据需要业务库与脱敏后的数据文件一一对应；

3. 脱敏主要通过数据库到数据文件的模式进行；

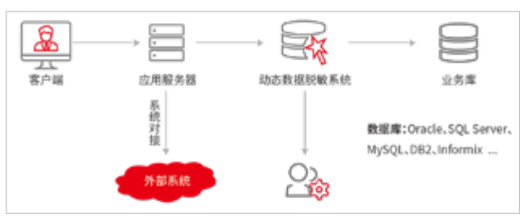
4. 可通过水印管理，对泄漏的数据进行快速溯源。

二、动态数据脱敏

动态脱敏则是相反的，一般是对数据进行实时脱敏，常用于对外提供访问接口的时候，外部可以访问数据，实时获取数据的场景。

亿赛通动态数据脱敏系统（简称 :DMS-D）是一款高性能、高扩展性的动态数据屏蔽和脱敏产品，在数据库通讯协议层面，通过 SQL 代理技术，实现了完全透明的、实时的敏感数据掩码能力；在不需要对生产数据库中的数据进行任何改变的情况下，依据用户的角色、职责和其他 IT 定义规则，动态的对生产数据库返回的数据进行专门的屏蔽、加密、隐藏和审计，确保业务用户、外包用户、运维人员、兼职雇员、合作伙伴、数据分析、研发和测试团队及顾问能够恰如其分地访问生产环境的敏感数据。

在应用侧，脱敏后的数据可以保留原有数据的特征和分布，无需改变相应的业务系统逻辑，实现了企业低成本、高效率、安全的使用生产的隐私数据；在运维侧，对敏感数据进行遮蔽处理，既不影响正常运维工作，又能够保证数据安全。



01、业务脱敏

老旧系统无法再做升级改造以及开发时未考虑数据隐私保护问题，重新修改代码过于复杂，只能依赖于外部技术实现数据的隐私保护。

1. 敏感数据自动发现，能大大减少了脱敏产品部署时用户的配置工作量，增强了系统的易用性；

2. 利用三层关联技术，可对不同业务帐号、不同业务模块配置脱敏策略，在业务系统本身无法限制业务人员查询信息时，可通过数据动态脱敏系统针对不同级别的业务人员进行权限管理，从而反馈不同的数据信息；

3. 无需对应用系统进行改造、无需修改数据库及存储数据，即可实现数据动态脱敏。

02、运维脱敏

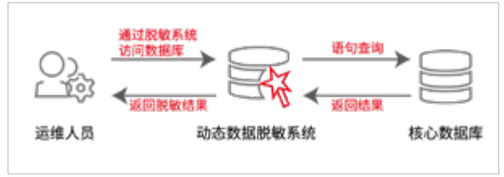
动态数据脱敏系统能有效的保障内部运维环境下的数据安全，防止敏感数据泄露。

1. 对于 DBA 等数据运维人员，可限制其在操作某些敏感表或越权操作其他数据表时返回的数据为非真实数据；

2. 对于运维人员恶意或失误进行高危或高风险操作时进行阻断，防止其危害数据库；

3. 支持透明网桥部署模式和本地代理模式；

4. 全面的审计记录：告警级别、事件发生时间、客户端 IP、目标数据库 IP、操作类型、客户端 MAC 地址 , 客户端端口号、返回状态、结果信息、客户端执行命令等。



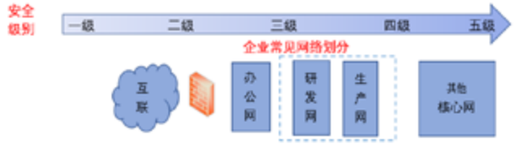
在面对具体的脱敏应用场景时，需要对一个完整的数据集进行脱敏，脱敏过程中还要保持数据的特性，保持数据特性之后才能从中挖掘出数据价值。数据脱敏可以在有效降低数据风泄露风险、保护数据安全的同时，不对数据的可用性产生影响，是既保证安全又挖掘数据价值的优选技术。

数据交换：如何搭建企业隔离网间的安全桥梁？

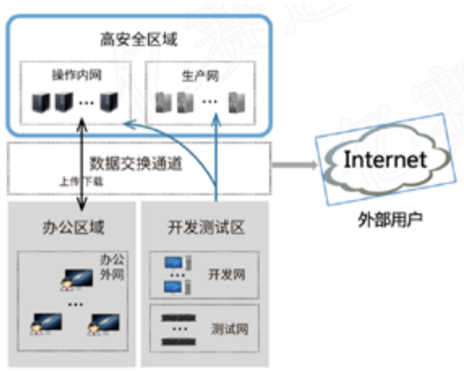
企业大量的 IT 投资建立了众多的信息系统，但是随着信息系统的增加，各自孤立工作的信息系统将会造成大量的冗余数据和业务人员的重复劳动。企业急需通过建立底层数据集成平台来联系横贯整个企业的异构系统、应用、数据源等，完成在企业内部以及其它重要的内部系统之间无缝的共享和交换数据。

在数字化转型的浪潮中，传统的隔离交换解决方案面临着数据量剧增、业务应用类型广泛以及信息泄露等诸多的风险，传统基于独立网闸设备实现数据隔离及交换的方案已无法满足企业需求，如何建立一种可靠、高效、动化的数据交换，已成为企业间资源共享，价值创新，实现优势互补重要课题。

在行业标准中明确要求，将企业网络按照不同的等级保护级别进行安全域划分，为了预防来自互联网的黑客攻击和病毒威胁，企业内部通常将网络划分为单独网络，即办公和生产网络之间做物理隔离。下图为企业内部网络通常的架构图：



该网络划分确实在一定程度上提升了安全等级，但无论是在业务还是管理层面，网络间的文件交互是必需的。所以实际上公司内部的网络拓扑如下图所示：



在这种情况下，存在的问题也随之暴露：

- 隔离网之间如何高效交换数据？
- 隔离网络中数据的安全性怎么得到保障？
- 交换过程是否安全可控？
- 交换过程时候可以审批？
- 交换行为是否安全可审计？
- 数据交换后能否防止敏感内容外泄？

当前市场上主流的隔离网络之间的文件交互是通过网闸技术来实现。即使用带有多种控制功能的固态开关读写介质，连接两个独立主机系统的信息安全设备。由于两个独立的主机系统通过网闸进行隔离，使系统间不存在通信的物理连接、逻辑连接及信息传输协议，不存在依据协议进行的信息交换，而只有以数据文件形式进行的无协议摆渡。因此，网闸从物理上隔离、阻断了对内网具有潜在攻击可能的一切网络连接，使外部攻击者无法直接入侵、攻击或破坏内网，保障了内部主机的安全。

而亿赛通的数据交换系统会部署在不同的隔离网络环境之间，为客户提供数据交换的一体化解决方案。产品集成安全隔离、访问控制、数据风险识别、交换过程审批、日志审计等多功能于一体，大幅提升隔离网络间的交换效率，实现高速、安全、可靠的信息交换服务。

01、网络安全隔离

使用信息摆渡技术的物理隔离卡，实现网络安全隔离效果。节点独立的管理机制，使隔离网络边界保持清晰，保证了系统架构的安全性。

02、跨网文件交换

不借助任何三方软件，在保证安全的前提下，提供文件方式的数据交换。支持交换方向的控制以及交换对象的选择。

03、数据泄露防护

系统采用完全自主开发的识别引擎，对文档数据进行深度识别和检测。有效防止涉密、敏感文件在未检测情况下的共享和使用。

04、用户访问控制

系统具有强大的访问控制能力，通过对用户行为细粒度的权限控制，轻松实现管理目标，保证文档在日常访问和交换过程中的内部安全。

05、交换行为审批

满足信息保护合规要求，支持数据外发过程中的审批操作。支持自动审批，人工审批，组合审批的多种审批形式。

06、交换过程审计

对交换行为、交换内容、审批行为、系统操作等进行详细的审计。有效帮助数据追根溯源，同时加强网络行为记录，提高数据资产安全。

企业内部核心隔离网为企业网络安全重点防护对象，保障核心隔离网络中的信息即保障公司业务的延续性，守护公司的核心资产，减少因信息安全时间带来的经济损失和负面影响，进而规避因信息泄露带来的法律风险，因此亿赛通诚挚希望能够协助各企业单位建立完善的核心网络防护体系。

基于数据分类分级的数据安全治理解决方案

10 月 25 日国家数据局正式揭牌，该机构由国家发展和改革委员会管理，主要负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等。这同时标志着我国数字经济发展新阶段的开始，预计数据要素配套政策将加快出台，数据要素产业进入加速发展期。

此前，《网络安全法》、《数据安全法》、《个人信息保护法》及各行业政策法规的相继出台实施，对如何建立科学全面的数据安全治理体系，更加有效地保障数据安全起到了指导性作用。支撑以数据为关键要素的数字经济发展，已成为国家、全社会以及政府部门、行业机构、企事业单位等各类组织需要面临的共同挑战。

企业的数据安全治理是企业综合考虑业务当前与未来发展需要，为保障数据安全所开展的一项系统工程。作为这一系统工程的相关方，各部门需要围绕企业的数据安全方针，就如何开展配合与协作、完善制度规范文件、部署安全技术产品、提升人员安全意识与能力。因此，为确保内部对数据安全治理的方针达成共识、合理配置数据安全工作任务与资源，需要建立企业层面的高层级决策、管理机构，使各部门、岗位人员明确其具体职责与分工。

从 Gartner 数据安全治理（DSG） 框架来看，数据安全治理是对数据获取、存储、分析、演变、归档、销毁等全生命周期的数据进行识别、分类与分级，并关注不同环节的安全风险点。数据分类分级是数据安全管理的基础性工作，最终目标是基于分类分级结果配置差异化的安全策略和技术保障手段，从而兼顾数据有序流动与安全保障。数据分类分级工作既需要国家层面根据数据重要敏感程度建立相应的保护制度，又要求行方全面落实数据分类分级管理工作，落实主体责任“三步走”，标准是国家、行业监管和指导企业落实数据分类分级管理工作的重要抓手 。

对数据安全治理而言，数据分类分级是基础保障性工作，亿赛通基于数据分类分级制定了完整的数据安全治理体系框架。从安全咨询服务到数据分类分级，最后进行数据分级管控。

开展组织架构建设时，需要考虑组织层面实体的管理团队及执行团队，也要考虑虚拟的联动小组，组织架构从上到下各部门均需要参与其中。除了人员配置外，完善的数据安全技术框架能够为数据安全治理提供可行性保障，企业在技术工具的布局与应用方面加强数据安全技术规划，防护布局由“点”向“面”趋势渐显。产品结合服务，将终端、数据库及文件服务器内的数据做梳理，完成结构化数据 + 非结构化数据分类分级，为数据分级管控做铺垫。最终形成数据资产清单，完成数据分类分级。

在亿赛通技术体系中，数据安全治理技术层借助于亿赛通数据安全运营管理平台，对企业个人隐私、核心业务等敏感数据进行识别定位，为后续针对关键数据和敏感数据的保护和治理工作提供明确目标；开放底层能力对接可实现接入数据安全防护系统；定位识别能力可实现合规和保护成果验证；运营层通过数据安全咨询服务，个性化定制分类分级规范及分级管控制度，完美展现产品 + 服务配置。

数据安全治理覆盖企业数据、业务、技术、管理等多个方面，是一项需要多方联动的复合型工作。企业应系统地进行数据安全治理能力建设，围绕数据的产生、加工、使用、流通、销毁等环节，进行总体布局、全面规划。企业可以构建贯穿各层面的数据安全治理组织架构，全面梳理业务场景并设计体系化的安全制度流程，配合应用自动化工具、平台，实现数据安全治理“一盘棋”。同时，企业通过搭建专业的人才梯队与培训机制，为数据安全管理工作持续积蓄力量。

为电力行业数据安全打下坚实基础

电力行业是国民经济基础性行业，能源电力安全是国家安全的重要组成部分，任何的数据泄露都可能会带来无法预估的损失。然而随着新兴技术入局，数据作为核心生产要素，逐渐集中、访问边界更加开放、使用方式越发复杂、数据权责已经分离，遭受安全威胁的暴露面不断增加，形势更为严峻。

国家能源局明确指出：要加快能源产业数字化智能化升级，推动能源基础设施数字化。同时要完善能源风险应急管控体系，强化重要能源设施、能源网络安全防护。同时，国家电网颁布一系列数据安全管理指导意见，针对电力行业，《国家能源局关于加强电力行业网络安全工作的指导意见》《泛在电力物联网全场景网络安全防护方案和互联网业务数据安全架构典型设计》《电力行业网络安全管理办法》《电力行业网络安全等级保护管理办法》等政策也提出明确要求。

由于数字电网概念的出现，由于电力企业数据安全建设过程中普遍存在以下问题：

数据更集中

业务域、管理域、网络域等各类数据集中存储，一旦发生安全事件则会波及海量客户敏感信息及公司数据资产的安全；数据库多部署于云环境中，由于存储、计算的多层虚拟化，带来了数据管理权与所有权分离、安全边界模糊等新问题。

业务系统更复杂

电力行业现有的信息化和安全防护设备种类繁多，安全策略配置、运维管理难度较大。当面对众多分散的信息时，安全人员无法快速、全面、直观地了解系统安全脆弱点、整体攻击状况以及安全防护效果。

运维人员更难管控

电力平台第三方建设及运维的网站较多，开放了很多核心数据库，重要数据直接暴露在第三方开发 / 测试人员面前，存在安全风险，并且当第三方在项目交付后，数据库账号没有及时收回，仍能随时访问重要数据，这也是安全风险之一。

数据对外共享更频繁

数据对外共享过程中，数据价值也不断增大，一旦发生安全事件，将对企业声誉、公司利益以及用户隐私产生重大损失及负面影响。

传统的信息安全建设无法覆盖现有的数据安全问题，因此电力企业需要数据安全治理思路体系化夯实安全防护能力。

围绕“让数据使用更安全”的目标，亿赛通重点关注数据的权限和使用场景，分阶段实现数据安全体系化建设。

短期大力开展数据安全治理、数据资产分级分类、数据安全风险评估、数据应用安全等领域相关工作，建立数据管理长效机制，夯实数据基础工作，支撑数据模型的运行。

中长期完善重点领域管理能力，管理体系完善建设，加强优化组织、制度、技术、人员闭环管理，推进数据管理各领域工作全面开展和数据安全管理能力全面提升，全面提升企业的数据安全建设成熟度。

基于数据安全解决方案框架，亿赛通在保证行业合规的基础上，对数据进行流转检测、事件溯源、风险评估、应急响应等手段。在数据的全生命周期中统一管控，做到数据安全态势一览，敏感信息识别、访问痕迹关联、数据分布监视、数据流向分析、数据访问分析数据流向告警等。从决策层到管理层再到执行层逐步完善宣贯。

电力安全无小事，数据安全本身的复杂性以及数据安全产品的碎片化导致数据安全建设落地的难度比较大，因此要有体系化思维，系统化作战，这也是电力企业未来数字化进程中应具备的基本能力，亿赛通基于沉淀的治理经验和产品能力，提供更为专业、全栈的产品与服务，助力电力企业数据更安全！

国网四川省电力公司信息通信公司

客户简介

国网四川省电力公司信息通信公司是国网四川省电力公司直属单位。国网四川信通公司于 2012 年 6 月 21 日成立，下设 4 个职能部门和 3 个业务机构。承担了特高压一级通信干线的属地化运维任务，以及三大特高压安控系统第二、三通道和直流控制保护业务二通道的通信传输任务。公司成立以来，为国网四川公司现代化管理、电网安全稳定运行提供了信息通信技术坚强支撑。在通信、信息领域取得多项重大科研成果，多次获得中国电力、四川省、国家电网公司、国网四川省电力公司科技创新一等奖。

典型案例 TYPICAL CASES

需求背景

国网四川信通公司创新管理模式，优化业务流程，构建了集约化、扁平化、专业化的信息通信体系，为了防止企业内部的财务、设计、市场等部门的重要资料在各种有意无意的情况下被泄露到企业外部，从而影响公司在行业中的竞争力，因而启动了数据安全防护项目。亿赛通对国网四川信通公司的现状进行了充分调研和论证，并最终决定按照根据其工作模式进行相关的部署和管理。

解决方案

1. 文档加密安全网关：通过加解密网关进行业务系统的安全保护，可使从业务系统上下载下来的文件经过加密处理，在企业内部可自由使用，泄露到企业外部无法使用。有效控制了业务系统流出文档的安全性。

2. 文档透明加密系统：实现了企业内部电子文件的加密存储。所有文件只要写在磁盘上就是加密形式；只有被系统授权许可，才可使用这些加密的文件，如未经合法许可将加密文件数据带走，加密文件内容将无法正常打开。透明加密，保护企业终端电脑办公文件安全，具有高适用性，灵活性。可根据客户需要调整安全等级，可自主设置加密解密。

项目成果

亿赛通提供的解决方案与国网四川信通公司的安全理念、安全需求高度融合，从根本上解决了企业存在的信息泄密隐患；通过高效先进的数据安全技术手段，解决了企业数据的存储、使用和传输中可能存在的泄密问题，帮助员工提高安全意识。